Council of the
European Union

Brussels, 27 September 2022
(OR. en)

12836/22

COVER NOTE

From:	Secretary-General of the European Commission, signed by Ms Martine DEPREZ, Director
To:	General Secretariat of the Council
No. Cion doc.:	SWD(2022) 308 final
Subject:	JOINT STAFF WORKING DOCUMENT **Sixth Progress Report on the implementation of the 2016 Joint Framework on countering hybrid threats and the 2018 Joint Communication on increasing resilience and bolstering capabilities to address hybrid threats**

Delegations will find attached document SWD(2022) 308 final.

Encl.: SWD(2022) 308 final

EUROPEAN
COMMISSION

HIGH REPRESENTATIVE
OF THE UNION FOR
FOREIGN AFFAIRS AND
SECURITY POLICY

Brussels, 16.9.2022
SWD(2022) 308 final

JOINT STAFF WORKING DOCUMENT

Sixth Progress Report on the implementation of the 2016 Joint Framework on countering hybrid threats and the 2018 Joint Communication on increasing resilience and bolstering capabilities to address hybrid threats

Sixth Progress Report on the implementation of the 2016 Joint Framework on countering hybrid threats and the 2018 Joint Communication on increasing resilience and bolstering capabilities to address hybrid threats

INTRODUCTION

Authoritarian regimes are increasingly trying to undermine the EU's democratic values using different hybrid tools, showing the importance of countering hybrid threats. Russia's unprovoked and unjustified ongoing war of aggression against Ukraine was preceded, and is accompanied, by hybrid activities targeting not only Ukraine, but also the West. Whilst countering hybrid threats remains predominantly Member States' responsibility, the EU can complement national actions by supporting coordination, enhancing situational awareness and resilience, cooperation with like-minded countries and organisations, and by providing joint response options in case of a hybrid campaign.

Conflicts and crises in our neighbourhood and beyond have a direct impact on our own security, while our political systems, societies and economies are increasingly targeted by sophisticated hybrid threats, including cyber-attacks and disinformation campaigns.

Our adversaries attempt to disrupt, divide, re-define the security architecture in Europe and challenge the international rules-based order. The EU faces more frequent cyber-attacks targeting our critical infrastructure, while foreign information manipulation and interference aims at the heart of our democracies. A striking development concerning hybrid attacks on the EU in the summer of 2021 was an attempt to destabilise the EU through the instrumentalisation of migrants at the EU external border.

Since 2016, the EU has set up a number of measures aiming for a holistic response across relevant instruments and actors to counter hybrid threats in a growing number of policy areas and has consistently adapted them to respond to ever-evolving hybrid activities. The progress made on the implementation of measures, announced in the **2016 Joint Framework on countering hybrid threats – a European Union response**[1] and further developed in the **2018 Joint Communication on Increasing Resilience and Bolstering Capabilities to Address Hybrid Threats**[2], carried forward in close interaction with Member States, EU institutions and entities, as well as with international partners, notably the North Atlantic Treaty Organization (NATO), was described in five annual progress reports[3].

Furthermore, the renewed EU approach to hybrid threats set out in the **EU Security Union Strategy 2020-2025**[4] of July 2020, is crucial for an effective policy to counter hybrid threats, bringing together the external and internal dimensions.

On 18 June 2020, the European Parliament decided to set up a **Special Committee on foreign interference in all democratic processes in the European Union**, including disinformation (INGE Committee). The INGE Committee delivered a report which was adopted by the European Parliament on 9 March 2022[5]. On 10 March 2022, the European Parliament set up a second Special Committee on foreign interference in all democratic

[1] JOIN (2016) 18 final
[2] JOIN (2018) 16 final
[3] JOIN (2017) 30 final; JOIN (2018) 14 final; SWD (2019) 200 final; SWD(2020) 153 final; SWD(2021) 729 final
[4] COM (2020) 605
[5] https://www.europarl.europa.eu/doceo/document/TA-9-2022-0064_EN.pdf

processes in the European Union, including disinformation (INGE 2), which will follow-up on the recommendations of the INGE Committee[6].

One of the most significant advances during the period under review was the approval of the **EU Strategic Compass for Security and Defence**[7] ("Strategic Compass"), which sets out an ambitious plan of action to increase the EU's capacity and willingness to act, strengthen our resilience and invest more and better in our defence capabilities. In the context of countering hybrid threats, the Strategic Compass announced the development of an EU hybrid toolbox, which will provide a framework for a coordinated response to hybrid campaigns affecting the EU and its Member States.

On 21 June 2022, the Council approved **Council Conclusions on a framework for a coordinated response to hybrid campaigns affecting the EU, Member States and partners**[8]**.** These Conclusions provide a framework for the development of the proposed EU hybrid toolbox and should also be used to address foreign information manipulation and interference (FIMI) in the information domain.

Complementary to the Conclusions above, on 18 July 2022, the Council approved **Council Conclusions on foreign information manipulation and interference** (FIMI)[9]. These Conclusions underline how FIMI is often used as **part of broader hybrid campaigns** and demonstrate the EU's commitment to strengthening its engagement to tackle this threat.

Furthermore, on 15 February 2022, the Commission announced a number of initiatives through its **Defence Package**[10] which will complement efforts in the area of hybrid threats.

This sixth progress report **takes stock of developments made since July 2021**. The report should be read in conjunction with the fourth progress report on the implementation of the EU Security Union Strategy[11] and the seventh progress report on the implementation of the common set of proposals endorsed by EU and NATO Councils[12].

IMPLEMENTATION STATUS OF THE 2016 JOINT FRAMEWORK AND THE 2018 JOINT COMMUNICATION ON COUNTERING HYBRID THREATS

Recognising the hybrid nature of a threat at the national level

In response to the December 2019 Council Conclusions on Complementary Efforts to Enhance Resilience and Counter Hybrid Threats[13] calling for a possible revision of the Hybrid Risk Survey in order to better address vulnerabilities to hybrid threats, Member States with the support of the Commission services and the European External Action Service (EEAS) launched a second Hybrid Risk Survey in December 2020, focusing on domains identified by Member States as of particular importance.

An important development was the inclusion of the EEAS, the Commission services and the General Secretariat of the Council contributions to the questionnaire. The importance of the

[6] https://www.europarl.europa.eu/doceo/document/TA-9-2022-0070_EN.html
[7] strategic_compass_en3_web.pdf (europa.eu)
[8] Council Conclusions on a framework for a coordinated EU response to hybrid campaigns, 603/22, 21 June 2022.
[9] Council Conclusions on Foreign Information Manipulation and Interference (FIMI), 11429/22, 18 July 2022.
[10] COM(2022) 60 final
[11] COM(2022) 252 final
[12] eu-nato-progress-report.pdf (europa.eu)
[13] EUCO 9/19

inclusion of relevant institutions was also reflected in the Council Conclusions on security and defence[14].

The final report on the second iteration[15], containing key findings and recommendations, was presented to the Horizontal Working Party on Enhancing Resilience and Countering Hybrid Threats on 12 November 2021, during the Slovenian Presidency. The discussions continued in February 2022, and the findings will guide future actions of the Council in the framework of this Horizontal Working Party.

EU Hybrid Fusion Cell (HFC)

At EU level, the HFC within the EU Intelligence and Situation Centre, is the **leading entity for building common understanding and comprehensive situational awareness on hybrid threats.** The HFC has continued to provide hybrid threat assessments to EU Member States, institutions, bodies and agencies. The HFC has presented **strategic, intelligence-based written and verbal briefings** to various Council formations. In support of the EU decision-making process, amongst other topics, the HFC has presented hybrid threat analysis and strategic foresight on Russia's ongoing war of aggression against Ukraine.

Through regular interaction with its multiple networks and partners, the HFC has continued its efforts to enhance a common understanding of hybrid threats at the European level. In the summer of 2021, the **list of the inter-institutional points of contact for the HFC was revised.** A wider range of subject-matter experts from the EEAS, the Commission and the Council was designated for exchanges with the HFC. The action is aimed at improving links between intelligence analysts and policy-makers, who can benefit from the cooperation in terms of building initiatives in response to hybrid threats, based on solid, comprehensive analytical background.

In cooperation with the rotating Presidency of the Council of the EU, the HFC **held bi-annual meetings of the national points of contact for countering hybrid threats**. In addition, within existing limitations of classified information sharing, it has maintained its **close cooperation with the NATO Hybrid Analysis Branch and partners**.

The importance of the HFC-led **Hybrid Trends Analysis** (HTA) has been acknowledged, in its latest iteration, by the **biggest participation of EU Member States and EU Institutions**, as well as very positive feedback by EU decision-makers[16]. The format of the classified report is now tailored for actor-based analysis and includes two new chapters – Hybrid Threats to the EU institutions and Hybrid Threats to the EU Common Security and Defence Policy (CSDP) Missions and Operations. At the request of the Member States, the HFC **shared its Concept of Hybrid Threats**. Multiple Member States confirmed that they have used the HFC concept as a guiding tool when preparing the national input for the HTA, which resulted in a significant increase in the quality of national contributions to the exercise. The next HTA will cover the year 2022 and will be issued in the beginning of 2023.

The HFC supported the preparation of the exercises EU MILEX-22 and the Integrated Resolve 2022. It was also actively involved in EU-wide cyber exercise CyCLES and Cyber

[14] Council Conclusions on Security and Defence, 10 May 2021, 8326/21.
[15] Analysis of the second iteration of the Hybrid Risk Survey, JRC 128513, Restricted
[16] The HTA was designed to inform EU decision-makers about the scale and intensity of hybrid threats targeting the EU, its institutions and Member States. It also offers an insight into potential escalation and future developments of the threats. It is based on voluntary contributions provided by relevant governmental, intelligence and security structures of the Member States, the EU Institutions and CSDP Missions and Operations.

Diplomacy Toolbox exercise, among others. In addition, the team continues to contribute to various events and trainings on hybrid threats with its expert knowledge.

Enhancing institutional resilience

The EU institutions, bodies and agencies (EUIBAs) have become highly attractive targets of sophisticated cyberattacks. Moreover, due to the interdependencies, technical links and close cooperation between the EUIBAs, any disruption to one of them could potentially result in far-reaching and long-lasting negative impact on the others. Thus, a common approach among all EUIBAs in the area of cybersecurity is more important than ever in order to enhance our institutional resilience.

To that end, on 22 March 2022, the Commission proposed **new rules to establish common cybersecurity and information security measures across the EUIBAs**. These rules will bolster the EU administration's resilience and ability to respond to cyber threats and incidents. By placing these activities in a common framework, inter-institutional cooperation will be strengthened, and risk exposure minimised.

The proposed **Cybersecurity Regulation for EUIBAs**[17] will put in place a framework for governance, risk management and control in the cybersecurity area and it will require EU institutions, bodies, offices and agencies to implement a baseline of cybersecurity measures addressing the identified risks. It will lead to the creation of a new inter-institutional Cybersecurity Board, boost cybersecurity capabilities, and stimulate regular maturity assessments and better cyber-hygiene. It will also extend the mandate of the Computer Emergency Response Team for the EU institutions, bodies, offices and agencies (CERT-EU), as a threat intelligence, information exchange and incident response coordination hub, a central advisory body, and a service provider.

The proposed **Information Security Regulation**[18] will create a standard set of information security rules and standards for all Union institutions, bodies, offices and agencies to ensure an enhanced and consistent protection against the evolving threats to their information. These new rules will provide a stable ground for a secure exchange of information across the European administration and with the Member States, based on standardised practices and measures to protect information flows.

Securing free and fair elections and protecting democratic processes

In November 2021, the Commission adopted **a package of measures to reinforce democracy and protect the integrity of elections**. The package includes a legislative proposal on the transparency and targeting of political advertising[19], a proposal to recast the regulation on the statute and funding of European political parties and foundations[20], two proposals to recast the directives on the voting rights enjoyed by mobile EU citizens in their Member State of residence in local and European parliamentary elections[21], as well as a Communication to protect election integrity and promote democratic participation[22].

[17] COM(2022) 122 final
[18] COM(2022) 119 final
[19] COM(2021) 731 final
[20] COM(2021) 734 final
[21] COM(2021) 733 final and COM(2021) 732 final
[22] COM(2021) 730 final

Cooperation among Member States to ensure resilient electoral processes and mutual support to address hybrid threats is essential. As announced in the **European Democracy Action Plan[23] and in the EU Citizenship Report 2020[24]**, the Commission continues to use the EU Network on Elections to deliver on a number of its commitments. Building on this cooperation, the Commission offers Member States a "joint mechanism for electoral resilience" as of 2022. It is organised and coordinated through the EU Network on Elections in close cooperation with the Network and Information Systems (NIS) Cooperation Group and the EU's Rapid Alert System (RAS). The mechanism's primary operational focus is to support deployment of joint expert teams and expert exchanges with the aim of building resilient electoral processes, in particular in the area of online forensics, disinformation and cybersecurity of elections.

Strategic communications

Foreign information manipulation and interference (FIMI), including disinformation, continued to pose a considerable threat to democracies and democratic efforts as well as to security around the globe in 2021. Therefore, the development of sound response options to tackle this threat remained a policy priority throughout the year.

The EEAS advanced its work on the development of policies, strategies and instruments to respond to FIMI and, in close cooperation with the Commission services, has been leading the efforts for the development of a **FIMI toolbox** and a common conceptual definition and analytical methodology, working closely with Member States as well as international partners, in particular the G7 and NATO. In this regard, the relevant work conducted in 2021 by the **European Parliament's INGE Committee** complemented the EEAS' work in assessing and exposing foreign actors and their tactics, techniques and procedures (TTPs) and again the need for a coordinated EU strategy against foreign information manipulation and interference.

The **Rapid Alert System** continued to share information and analysis on a daily basis, and allowed for exchanges with G7 Members and NATO International Staff. In addition to the overall situational awareness, Members contributed to the debates on the policy framework to tackle foreign information manipulation and interference as well as potential joint approaches and responses.

The pandemic showcased the Commission's ability to deploy strategic communication in supporting Member States' efforts to swiftly distribute vaccines, communicating on their benefits, convincing citizens of the importance of getting vaccinated, while tackling mis- and disinformation in the context of the EU's Vaccines Strategy. In addition, the Commission's communication strategy enforced the message concerning confidence in vaccine health benefits, the authorisation process at EU level and the safety and efficacy of COVID-19 vaccines. Furthermore, the Commission implemented a series of targeted campaigns, notably targeting countries with relatively low uptake of vaccination.

The exposure of FIMI activities in the EU's neighbourhood was further strengthened in 2021 through the work of the **three EEAS Stratcom Taskforces, supported by the 27 regional stratcom officers.** Awareness raising on actions conducted by the Kremlin and other state/non-state actors was complemented by proactive communication based on facts, in local languages, and in collaboration with local stakeholders from the **Eastern Partnership** (EaP),

[23] COM(2020) 790 final
[24] https://ec.europa.eu/info/sites/default/files/eu_citizenship_report_2020_-_empowering_citizens_and_protecting_their_rights_en.pdf

the **Western Balkans**, the **Middle East and North Africa** (MENA) as well as **Sub-Saharan Africa**. The work to support events such as the **Eastern Partnership Summit, the EU-Western Balkans Summit, and the Conference on the Future of Europe** reconfirmed the commitment to building local and regional partnerships with civil society activists, fact checkers, opinion leaders, governments and journalists to counter FIMI, promote civic engagement and activism, and support a vibrant media environment which can serve as inspiration both locally and globally.

With a threat landscape evolving both in intensity and in sophistication across Sub-Saharan Africa, the EEAS stepped up its work on supporting the **CSDP missions and operations,** through the reinforcement of their situational awareness and capacity building elements for adequate response to such threats.

The COVID-19 pandemic and related FIMI also highlighted the need to strengthen the EEAS' response to information manipulation and interference by the Chinese actors. In 2021, the EEAS continued to build its expertise and engaged with international stakeholders on these particular actors.

The Commission worked to reduce the threat of disinformation through the **Code of Practice on Disinformation**[25]. In line with the 2020 European Democracy Action Plan, the Commission published a Guidance in May 2021[26] setting out its views on how the Code should be further adapted to be fit for purpose. On 16 June 2022, the Code's signatories and potential new signatories completed a thorough revision and strengthening of the Code following the Guidance.

Several positive developments have been achieved under the current edition of the Code. The signatories to the Code have put in place policies aimed at reducing opportunities for advertising placements and economic incentives for actors that disseminate disinformation online as well as enhancing transparency of political advertising, by labelling political ads and providing searchable repositories of such ads. They have also taken action against malicious actors' use of manipulative techniques on platform services and set up technological features that give prominence to trustworthy information.

It is envisioned that the Code will be transformed into a "Code of Conduct" under the **Digital Services Act** (DSA)[27]. This means that for very large online platforms, the Code will be a means to meet their risk mitigation obligations once the DSA enters into force.

The EU Research and Innovation Framework Programme for the period 2021-2027 under Horizon Europe, has enabled the Commission to continue to fund innovative research to empower citizens to make informed decision. Under its first calls launched in 2021 for the cluster "Civil Security for Society", the programme will support research on politics and the impact of online social networks and new media, on combatting disinformation and fake news and restoring trust in the digital world, and on tools to fight disinformation based on artificial intelligence.

The Commission is also continuing to support the work of the **European Digital Media Observatory** (EDMO), which is creating a cross-border and multidisciplinary community of independent fact-checkers and academic researchers in the EU. EDMO comprises a central digital platform, governed by an independent board composed of experts in relevant fields that interconnect with national and regional research hubs. The hubs leverage their specific knowledge of local information environments in order to better focus detection and analysis

[25] https://digital-strategy.ec.europa.eu/en/policies/code-practice-disinformation
[26] COM(2021) 262 final
[27] COM(2020) 825 final

of disinformation threats and trends across Europe. The Commission has provided grants for a total amount of EUR 11 million to establish eight EDMO regional hubs[28]. The Commission has issued a call for proposal for further grants to regional hubs, with the aim of expanding coverage to 100% of the EU population.

The Joint Communication "Tackling COVID-19 disinformation - Getting the facts right"[29] of 10 June 2020 set out a reporting and monitoring programme under which the platform signatories to the Code of Practice have been reporting on monthly basis since July 2020 on actions taken to counter disinformation around the crisis. Throughout the course of the programme, the Commission has been in close contact with the platforms to ensure that the Code's safeguards are being effectively applied. All platforms - depending on the nature of their services - have increased the visibility of authoritative sources by giving prominence to COVID-19 information from the World Health Organization and national health organisations, and by deploying new tools and services to facilitate access to relevant and reliable information relating to the evolution of the crisis. The reports also highlight how the platforms have taken action against a vast amount of content containing false or misleading information, in particular by demoting or removing content liable to cause physical harm or impair public health policies, in violation of their terms of service.

In response to the unprecedented crisis regarding Russia's war of aggression against Ukraine, the Commission services and the EEAS have been holding regular and ad-hoc discussions with the platform signatories of the Code of Practice (Alphabet, Meta, Twitter, ByteDance, Microsoft) to discuss **disinformation and information manipulation linked to Ukraine**. These meetings are monitoring the implementation of the EU restrictive measures related to Russia Today and Sputnik, Rossiya RTR/RTR Planeta, Rossiya 24/Russia 24 and TV Centre International and mapping the situation on the ground. Overall, platforms have not reported significant information manipulation actions (i.e. inauthentic coordinated behaviour) but an increased spread of narratives and war propaganda by Russian state-affiliated media and actors spreading such narratives for economic gain. The Commission called on the platforms to step up their efforts, in line with the Code of Practice, to address the spread of war propaganda and harmful disinformation related to the war[30]. The Commission keeps monitoring progress in these areas.

As regards the most recent efforts to reach out to Russian speaking audiences, the Commission has put in place several actions on social media communication ("EU Neighbours East" regional communication programme has included Russian on all communication on various social media channels).

The communication response to disinformation is coordinated through the Commission's internal Network against Disinformation. The Commission has been working to tackle disinformation and misinformation within the Union and in its neighbourhood enhancing its strategic communication efforts, providing positive messages and factual information in close coordination with representations, delegations and Europe Direct centres. The EEAS has taken action to step up response around the world, providing guidance and communication products to EU delegations, for proactive outreach, as well as to counter narratives spread by state and non-state disinformation actors in their local and regional context.

[28] Covering Ireland, Belgium, Czechia, Denmark, Finland, France, Italy, Luxembourg, the Netherlands, Poland, Slovakia, Spain, Sweden, as well as Norway.
[29] JOIN(2020) 8 final
[30] In particular, the Commission asked platforms to i) increase labelling, demotion or removal of debunked information or deceptive manipulated material; ii) ensure more prompt and consistent closure of accounts that are persistently disseminating disinformation related to the war; iii) adapt recommender systems in particular to promote authoritative sources; and iv) reduce monetisation/advertising opportunities for malicious actors.

European Centre of Excellence for Countering Hybrid Threats (Hybrid CoE)

The Hybrid CoE, founded in 2017 and based in Helsinki, has continued to grow and expand its networks and the scope of its activities. As of April 2022, the Centre had **31 Participating States which are members of the EU and/or NATO**[31]. The Hybrid CoE continues to support its Participating States and two major stakeholders, the EU and NATO, by providing educational events, trainings, exercises, seminars, workshops, publications, and conferences on hybrid threats.

Despite the ongoing pandemic, the Centre has supported more than 17 exercises organised by the EU, NATO, and the Participating States. The "Hybrid 101" introductory course has been offered to the Commission and other EU institutions with the first two courses conducted so far on 26 January 2022 and 5 May 2022.

The Hybrid CoE has supported the rotating presidencies of the Council of the EU in the framework of the Horizontal Working Party on Enhancing Resilience and Countering Hybrid Threats and by organising joint events and seminars on topical issues, such as the use of instrumentalised migration by Belarus in 2021.

Last year, the Centre's experts also contributed to the policy discussions around the Strategic Compass on multiple occasions. The Centre's role as a neutral space for dialogue between the EU and NATO has helped to build and maintain common understanding of hybrid threats in the two organisations.

The Hybrid CoE has continued its close cooperation with the Commission's Joint Research Centre (JRC) with a joint project focusing on resilience against hybrid threats "Hybrid Threats: A Comprehensive Resilient Ecosystem (CORE)". The project aims to present a European resilience ecosystem model that allows strategic assessment of the impact of hybrid threats and devising effective responses to them. A draft of the final report was presented to the Horizontal Working Party in February and May 2022. The report was published on 4 July 2022.

The partnership with the JRC extends to the Horizon 2020-funded **EU-HYBNET** network, which brings together European security practitioners, academics, industry players and small and medium-sized enterprises engaged in addressing hybrid threats. The five-year project entered its second 18-month cycle in October 2021, and will be hosted by the Hybrid CoE after the term ends.

Hybrid CoE's cooperation with the European Defence Agency (EDA) has continued, including in the context of the EDA-led Cyber Phalanx 2021-exercise in late 2021.

Protection of critical infrastructure

Further progress was made on the updated legislative framework for resilience, including against hybrid threats. The proposal for a **Critical Entities Resilience (CER) Directive** was announced in the EU Security Union Strategy and published in December 2020[32]. A political agreement was reached by co-legislators in June 2022. The agreement covers critical entities in a number of sectors, such as energy, transport, health, drinking water, waste water, space,

[31] The most recent States to join were Croatia, Belgium and Iceland, and more countries are expected to join.
[32] COM (2020) 829 final

along with central public administrations in some of the provisions of the draft Directive. The CER Directive covers natural and man-made non-cyber threats, including terrorism sabotage, infiltration and will complement the **Directive on measures for high common level of cybersecurity across the Union (NIS-2 Directive)**[33]**,** which places cybersecurity requirements on operators in a number of critical sectors, revising the current NIS Directive. Both directives combined will provide a coherent and comprehensive framework for resilience in many dimensions of hybrid threats.

Under the **European Programme for Critical Infrastructure Protection** (EPCIP), Member States and the Commission continued cooperation on various aspects to enhance resilience of critical infrastructure. For that purpose, discussions related to hybrid threats were part of the 2022 meeting of the Commission Critical Infrastructure Protection Expert Group (CIP Points of Contact). EPCIP also includes cooperation with third countries. In line with this, the series of annual expert meetings with the United States and Canadian authorities continued in 2021 and 2022.

The EU budget has been triggered to fund resilience to hybrid threats under security research in sectors such as energy, space, water, health, transport, communication and finance. Ten Horizon 2020 projects from the Secure Societies cluster with a combined EU contribution of around EUR 77 million support infrastructure resilience. Among those is the project 7SHIELD that deals with the resilience of ground segments of space infrastructure and the project EU-HYBNET that brings together practitioners and stakeholders to identify and define their most urgent requirements for countering hybrid threats. Another example is the EU Horizon 2020 SATIE project, aimed at providing a holistic security solution that protects critical air transport infrastructures and aviation systems against combined cyber-physical threats. Furthermore, under the first work programme of Horizon Europe, funding was allocated for a flagship project on countering hybrid threats against critical infrastructure, and resilience of critical infrastructure is a priority in the first security research programme, with a dedicated call for proposals worth EUR 10 million to counter hybrid threats[34].

In the context of the **European Reference Network for Critical Infrastructure Protection (ERNCIP)**, on 11 January 2022, the Thematic Group on Chemical and Biological (CB) Risks to Drinking Water published the "Water Security Plan - Implementation Manual for Drinking Water Systems"[35] which helped to identify security vulnerabilities and establish security measures to detect the intentional contamination of water supply systems, including a communication strategy to facilitate a fast and effective response.

The provisions on the EU's **disaster resilience goals** in the revised EU Civil Protection Mechanism (UCPM) legislation was adopted in May 2021. These are explicitly limited to the area of civil protection and are adopted in the form of Commission recommendations as "non-binding common baseline" objectives to support prevention and preparedness action. The legislation does not lay down the goals themselves but calls on the Commission and Member States to work together to develop them. In July 2021, the first exchanges on disaster resilience goals took place in a Slovenian presidency workshop. Technical work with national experts started in September 2021. The adoption of the first Commission Recommendation on disaster resilience goals is planned for December 2022.

In the framework of the European Union Maritime Security Strategy (EUMSS), the Commission promotes an enhanced overall **resilience of EU critical maritime**

[33] COM (2020) 823 final
[34] HORIZON-CL3-2021-INFRA-01-01: European infrastructures and their autonomy safeguarded against systemic risks
[35] https://erncip-project.jrc.ec.europa.eu/sites/default/files/JRC126684_01.pdf

infrastructure by assessing and improving the resilience of critical maritime transport infrastructure, such as port security, sea lines of communication, energy infrastructure, offshore installations and telecommunications networks and sensors (e.g. cables), including under water. In 2021, the Commission services and EEAS carried out an assessment of the EUMSS and determined the need for an update, which they started working on in the first quarter of 2022.

Energy security of supply and energy infrastructure

With respect to **nuclear energy**, the Commission and the Euratom Supply Agency (ESA) continued to recommend that utilities take concrete action in relation to the emergence of alternative nuclear fuel designs or suppliers. ESA is closely monitoring steps towards supply diversification of fuel for VVER-1000 reactors (Russian-designed) in Czechia and Bulgaria as well as the medium/long-term plans of major EU fuel manufacturers. The Commission addressed issues relating to security of supply in the final national energy and climate plans (NECP) prepared by Member States for 2021-2030 and gave recommendations relating to security of supply of nuclear materials and diversification policies.

With regard to **electricity security of supply**, in January 2022, Member States adopted their first Risk-Preparedness Plans containing measures to prevent and mitigate identified risks. These plans are based on regional and national electricity crisis scenarios that consider, among others, consequential hazards including the consequences of malicious attacks and of fuel shortages. The Commission is assessing these plans, in accordance with Regulation 2019/941 on risk-preparedness in the electricity sector[36], and putting forward a number or recommendations[37] focussing on changes to the EU security situation resulting from the Russian's war of aggression against Ukraine, notably the need to update plans in the light of such circumstances, to run tests ahead of winter and to develop, as a matter of urgency, the cooperation and assistance mechanism established by Regulation 2019/941. The latter requires Member States to offer assistance to each other to prevent or manage electricity crises.

Concerning **gas security of supply**, on 8 March 2022, the Commission presented the **REPowerEU communication**[38] as a reaction to Russia's war of aggression against Ukraine, which calls for a phase out of Russian fossil fuels, including gas. Moreover, on 18 May 2022, the Commission adopted a concrete REPowerEU Plan[39] to implement such a phase out, as requested by the European Council at its meeting in March 2022. The measures in the REPowerEU Plan address energy savings, the diversification of energy supplies, and an accelerated roll-out of renewable energy to replace fossil fuels in homes, industry and power generation. The Commission also adopted a **storage proposal**, which would require Member States to have gas storage levels up to 80% in 2022 and 90% in subsequent years. Coordination with Member States and organisations such as the European Network of Transmissions System Operators for Gas (ENTSOG) continues through increased efforts in the Gas Coordination Group. Cooperation through this Group was also instrumental to coordinate efforts to create a reinforced risk preparedness analysis, which earlier this year analysed different gas disruption scenarios during the past winter. This analysis will be updated to assess the EU's immediate preparedness to a potential large-scale gas disruption.

[36] OJ L 158, 14.6.2019, p. 1-21.
[37] https://energy.ec.europa.eu/topics/energy-security/security-electricity-supply/risk-preparedness-plans-electricity-sector-national-competent-authorities-and-commissions-opinions_en
[38] COM(2022) 108 final
[39] COM(2022) 230 final

Since 18 May 2022, REPowerEU has been working with international partners to diversify supplies and has secured record levels of LNG imports and higher pipeline gas deliveries. The newly created EU Energy Platform[40], supported by regional task forces, enables voluntary common purchases of gas, LNG and hydrogen by pooling demand, optimising infrastructure use and coordinating outreach to suppliers.

The **Consultation Forum for Sustainable Energy in the Defence and Security Sector** (CF SEDSS), the Commission funded initiative managed by the EDA, continued to address energy security challenges, including the protection of defence-related critical energy infrastructure (CEI).

Transport security

For all the areas of transport, namely civil aviation, maritime transport and land transport, the Commission, together with the relevant agencies, maintains a continuous dialogue on emerging security threats, including those of a hybrid nature, with Member States and Contracting Parties to the Agreement on the European Economic Area, industry and other stakeholders**.** Ensuring that the transport system is truly resilient to future crises is a key objective of the EU's transport policy.

Since the beginning of **Russia's war of aggression against Ukraine**, the Commission has taken a proactive approach to manage the situation in terms of security risk for critical transport infrastructure. In the maritime sector, shortly after the start of Russia's war of aggression against Ukraine, the European Maritime Safety Agency (EMSA) started producing daily reports with the detailed situation at sea, in the affected areas of the Azov Sea and the Black Sea, identifying all merchant ships sailing in those areas and in ports, with the focus and providing data on EU-flagged vessels and those carrying hazardous materials (Hazmat). Moreover, actions and measures to be deployed to ensure safe and secure navigation and shipping operations in this area were discussed at the International Maritime Organization (IMO) Council meeting. Similarly, in the aviation sector, the Commission and European Union Aviation Safety Agency (EASA) have been closely monitoring the security risk to civil aviation, even before the start of Russia's war of aggression. On 24 February 2022, EASA, in close cooperation with the Commission and Eurocontrol, issued a Conflict Zone Information Bulletin (CZIB) recommending that EU operators do not operate within the airspace of Ukraine, Moldova and the airspace within 200 nautical miles surrounding the borders with Ukraine. The war has intensified Global Navigation Satellite Systems (GNSS) jamming and/or possible spoofing in geographical areas surrounding Ukraine and other areas[41] which the Commission is closely monitoring. Recent incidents have also highlighted the potential overspill of the armed conflict in Ukraine into the airspace over its neighbours to the west, primarily EU Member States[42]. Increased military air operations, including uncontrolled drones, have the potential to cause airspace congestion and impact the safety and security of civil aviation flights.

The Commission adopted the Communication on the **Contingency Plan for Transport** on 23 May 2022[43]. Amongst others, the plan focuses on raising the resilience and preparedness of

[40] https://ec.europa.eu/commission/presscorner/detail/en/IP_22_2387

[41] Namely the Kaliningrad region, surrounding Baltic Sea and neighbouring states; Eastern Finland; the Black Sea; and the Eastern Mediterranean area near Cyprus, Turkey, Lebanon, Syria and Israel, as well as Northern Iraq.

[42] On 10 March 2022, a drone crashed in the southwest of the Croatian capital, Zagreb. It was subsequently identified as a Soviet-era Tu-141 military drone, known to be operated by the Russian and Ukrainian military.

[43] COM(2022) 211 final

the transport sector to increasingly present hybrid threats in order to avoid disruptions to the transport system and preserve the integrity of the Single Market.

In the **area of land transport security**, the Commission has continued to support the exchange of relevant experience, policies and best practices[44].

In the **area of rail security,** decisive progress was made in recent months by the Commission towards the full implementation of the 2018 Action Plan to improve the security of rail passengers and staff[45]. In July 2021, the Commission established a new Working Party on Rail Security under the umbrella of the Expert Group on Land Transport Security. As an example, it is currently developing guidelines on security culture that will be completed in the second half of 2022.

In the area of **maritime and aviation security**, the Commission has established common rules and standards aimed at protecting aviation and maritime infrastructures from unlawful interference.

In the **aviation sector**, the Commission continued to carry out its regular monitoring of emerging threats, including hybrid threats, to adapt the Aviation Security (AVSEC) baseline. The Commission also continued to ensure a high level of protection of civil aviation against acts of unlawful interference, supported by the Commission aviation security inspections system. In 2021, despite the constraints linked to the COVID-19 pandemic, the Commission continued inspections of national administrations of Member States in accordance with its inspection strategy, using remote methods.

Unmanned aircraft systems (UAS, or drones) have the potential to be used by different malicious actors, including the ones involved in hybrid actions, to conduct surveillance, disrupt critical infrastructure operations or attack high-value targets. The Commission is engaged in supporting Member States in countering such misuse through a number of measures. The Commission is taking additional steps, such as financing innovative counter-drones projects and studies, and building bridges between different affected sectors (e.g. law enforcement, aviation, critical infrastructure, prisons, customs/borders, personal protection, mass events) and stakeholders. Besides Member States authorities, these include third countries, international organisations, industry, academia and civil society.

On **maritime security**, the Commission continued to monitor conflict events or situations that could impact maritime security, including piracy and maritime disputes, and that could disrupt shipping and trade routes of EU interest.[46]

The Commission services, the EEAS and the EDA continued to support a coordinated response to hybrid threats affecting people, activities, and infrastructure in the maritime domain under the framework of the EU Maritime Security Strategy and its Action Plan.

In line with the Council Conclusion on maritime security of 22 June 2021[47], the Commission, in close cooperation with EMSA, is developing the Common Information Sharing

[44] LANDSEC, the Expert Group on Land Transport Security, assists the Commission in formulating and implementing the European Union's activities aimed at developing policy on security relating to land transport, and to foster ongoing exchanges of relevant experience, policies and practices between the Member States and the various parties involved.

[45] https://ec.europa.eu/transport/modes/rail/news/2018-06-12-action-plan-security-railpassengers_en

[46] The Commission closely monitored UNCLOS/international law compliance, maritime disputes and maritime incidents, with a possible or effect on EU interests or risk of potential disruption, mainly regarding the freedom of navigation in the current (or future) international shipping routes; including developments in the South China Sea, Taiwan Strait, the gradually opening Northern Sea Route and the trans-Arctic routes, or the lasting sabotage attacks and maritime incidents in the HoA/Gulf of Aden, around the strategic Bab-el-Mandeb Strait.

[47] Council Conclusions on maritime security, 9946/21, 22 June 2021.

Environment (CISE) for the maritime domain, as a network to facilitate the interoperability and the exchange of information between different authorities in charge of maritime surveillance (defence, customs, border control, general law enforcement, fisheries control, marine environment protection, maritime security and safety). CISE is an essential tool to enhance maritime situational awareness, as well as to identify, monitor and respond to possible hybrid threats.

Furthermore, the Commission continued to engage with stakeholders and Member States to improve passenger ship security and finalised a methodology for an EU-level risk assessment exercise on passenger ship security.

The Commission, supported by its Maritime Security Inspection system, also ensured that ships, ports and port facilities (port terminals) in the EU are properly secured and protected. In 2021, despite the constraints linked to the COVID-19 pandemic, the Commission was able to resume on-site inspections in Member States in accordance with its inspection strategy[48].

In parallel, EMSA kept on supporting the Commission and the Member States in various tasks notably within the Maritime Security Committee (MARSEC) and the Stakeholders Advisory Group on Maritime Security (SAGMAS). The first version of the interim Guidance on Maritime Security prepared jointly by the Commission and EMSA was adopted during the 83rd MARSEC Committee meeting on 9 September 2021. EMSA also worked on a thorough study on remote surveys, inspections and verifications in the field of maritime security in order to maintain the appropriate security level even in times of pandemic.

Regarding Maritime Surveillance (MARSUR), further development of the MARSUR project was ensured by EDA to improve exchange of maritime surveillance data in the defence sector and contribute to cooperation in the Common Information Sharing Environment (CISE) framework.

Transport and logistics were identified as recurrent bottlenecks in EU Civil Protection Mechanism (UCPM) response operations over the past years (Afghanistan, COVID-19 transport of medical assets, vaccines, personnel and patients or more recently transport and MEDEVAC in the context of the Russian aggression in Ukraine). The subjects of transport and logistics were included as the fourth area for European reserve of additional capacities (the "rescEU" reserve) in the UCPM legal basis, which was revised in 2021. Following discussions with Member States' experts, an implementing act on quality requirements was adopted on 15 March 2022[49]. Subsequently, a call for proposals for the development and maintenance of rescEU transport and logistics capacities was launched in June 2022.

Border and supply chain security

The inter-agency cooperation **in support of coastguard function activities** between the European Fisheries Control Agency (EFCA), the EMSA and the European Border and Coast Guard Agency (FRONTEX) is ongoing in a number of areas[50]. The main aim of this cooperation, in line with the EUMSS Action Plan is to assist national authorities in the performance of their coast guard functions.

[48] In 2021, the Commission carried out 12 maritime security inspections in 11 Members States.

[49] Commission Implementing Decision (EU) 2022/461 of 15 March 2022 amending Implementing Decision (EU) 2019/570 as regards rescEU transport and logistics capacities (notified under document C(2022)1685), OJ L 93, 22.3.2022, p. 193–196.

[50] Namely, information sharing; surveillance and communication services; capacity building; risk analysis; and capacity sharing.

In December 2021, the Commission proposed updated rules to **reinforce the governance of the Schengen area**[51]. The proposed changes to the Schengen Border Codes aim at bringing greater EU coordination and to better equip Member States to deal with emerging challenges when managing both the EU's common external border and internal borders within the Schengen area. The instrumentalisation of migration, which is a phenomenon of increasing importance and one of growing concern for the EU, is also addressed in the update to the Schengen rules, as well as through a parallel proposal for measures Member States can take in the fields of asylum and return in such a situation[52].

The EU is taking steps to enhance its Export Control System. In particular, the EU adopted a new **Dual-Use Export Control Regulation** in May 2021[53], which entered into force on 9 September 2021. This Regulation provides a comprehensive improvement of export control rules to make them more efficient and introduces new provisions for the EU to tackle more efficiently the challenges associated with trade in dual-use cyber-surveillance technologies and emerging technologies. In addition, the Commission, in cooperation with Member States in the Dual Use Coordination Group, has published adopted guidelines on internal compliance programmes for controls of research involving dual-use items on 15 September 2021[54]. The EU is also working with the Member States to develop guidelines on the export of cyber-surveillance items and is implementing actions to further develop the IT infrastructure that supports the implementation and enforcement of controls of dual-use items. Furthermore, the EU is extending cooperation with partners and allies, in particular with the US in the Trade and Technology Council, to address global trade and technology challenges while upholding international security and ensuring a level-playing field.

Following Russia's war of aggression against Ukraine, the EU, in close coordination with its allies, has also adopted a set of sweeping sanctions, including restrictions to export to Russia and Belarus of dual-use and advanced technologies that undermine Russia's capability to continue the war.

In the area of **supply chain security**, the Commission published the Annual Single Market Report[55] on 22 February 2022. The report responds to a renewed attention to the importance of **strengthening the resilience of the Single Market**. In particular, it confirms the importance of the effective implementation and enforcement of the Single Market rules and a well-functioning Single Market to enhance the security of supply also in times of crisis. At the same time, it points to the need to reinforce the resilience of supply chains and of the Single Market in order to reduce negative impacts of supply challenges on economic activity and trade. To this end, it shows the approach taken by the Commission during the COVID-19 pandemic to secure the supply of personal protective equipment and ramp up the industrial production of vaccines as examples of action to address severe supply risks relating to products of strategic importance.

Furthermore, the Commission has been dealing with **performance requirements for threat detection equipment used in public spaces and explosives precursors**. On explosives

[51] COM(2021) 891 final
[52] JOIN(2021) 32 final
[53] Regulation (EU) 2021/821 of the European Parliament and of the Council of 20 May 2021 setting up a Union regime for the control of exports, brokering, technical assistance, transit and transfer of dual-use items (recast), OJ L 206, 11.6.2021, p. 1-461.
[54] Commission Recommendation (EU) 2021/1700 of 15 September 2021 on internal compliance programmes for controls of research involving dual-use ítems under Regulation (EU) 2021/821 of the European Parliament and of the Council setting up a Union regime for the control of exports, brokering, technical assistance, transit and transfer of dual-use ítems, OJ L 338, 23.9.2021, p. 1-52.
[55] SWD(2022) 40 final

precursors, the Commission gives science-based advice and performs experimental work for the Standing Committee for Precursors (SCP), in support of Regulation 98/2013 on explosive precursors[56].

Furthermore, the Commission has published a **toolkit**[57], in collaboration with Member States and research and innovation stakeholders, on how to **mitigate foreign interference in research and innovation.** The publication outlines best practices to support EU higher education institutions and research performing organisations in safeguarding their fundamental values, including academic freedom, integrity and institutional autonomy, as well as to protect their staff, students, research findings and assets. It will help them to develop a comprehensive strategy for tackling risks and challenges from abroad that covers values, governance, partnerships and cybersecurity.

Space

In 2021, Copernicus continued supporting the resilience and security of the EU and its Member States, and countering hybrid threats, with the provision of its **security service** (including border surveillance, maritime surveillance and support to EU external action) and its **emergency management service** (for civil protection in case of natural or man-made disasters). More generally, considering also its several environmental services, Copernicus reinforces the EU sovereign access to relevant Earth-observation data in support of situational awareness, preparedness, response and independent decision-making in times of threats and crisis. Moreover, the Commission is preparing the implementation of new Copernicus security requirements stemming from the Union Space Programme Regulation adopted in 2021, which will reinforce the security of Copernicus, notably with regards to cyber-attacks.

In February 2022, the Commission adopted the proposal for a Regulation establishing the **Union Secure Connectivity Programme for the period 2023-2027**[58]. The objective of the initiative is to build and operate a multi-orbital space-based state-of-the-art connectivity system, able to adapt to satellite communications demand evolution that would ensure worldwide access to secure satellite communication services for protection of critical infrastructures, surveillance, external actions and crisis management. The system developed under this programme will increase cyber resilience by defending against cyber threats, provide strong encryption capability with the integration of the space European Quantum Communication Infrastructure, thereby improving the resilience of the Union telecommunication infrastructures.

An effective extension to cover a wider range of threats would need a strong increase of performance, of the number and the geographical repartition of sensors, and probably additional space-based sensors in order to improve reactivity. The Joint Communication "**An EU Approach for Space Traffic Management (STM)**[59]" also adopted in February 2022, allows progress in this direction by aggregating civilian and military requirements towards an EU STM approach, and by supporting the improvement of existing space surveillance and tracking services.

[56] Regulation (EU) No 98/2013 of the European Parliament and of the Council of 15 January 2013 on the marketing and use of explosive precursors, OJ L 39, 9.02.2013, p. 1-11.
[57] https://op.europa.eu/en/web/eu-law-and-publications/publication-detail/-/publication/3faf52e8-79a2-11ec-9136-01aa75ed71a1
[58] COM(2022) 57 final
[59] JOIN (2022) 4 final

Defence capabilities

The Strategic Compass reaffirmed the need to develop next generation capabilities and committed to taking forward the recommendations of the first-ever **Coordinated Annual Review on Defence** (CARD) Report, including the agreed six capability focus areas that would benefit from enhanced defence cooperation among Member States[60]. Some of these activities, for example the ones brought forward by the "Enhanced Military Mobility" focus area, take into account threats that are of hybrid nature. Collaborative opportunities in areas as cyber defence, counter improvised explosive devices (C-IED) and explosive ordnance disposal (EOD), harbour protection and counter unmanned aerial systems (C-UAS) will overall contribute to enhancing our resilience and ability to counter threats of a hybrid nature.

The **Permanent Structured Cooperation** (PESCO) also contributed to the efforts of countering hybrid threats through the fulfilment of the more binding commitments, as agreed by the participating Member States, as well as the projects, which are being implemented in the PESCO framework. The set of more precise objectives of PESCO was revised in 2021 where countering hybrid threats was indicated as one of the areas where further attention on collaboration by participating Member States is required. In terms of projects, a new project called "Cyber Ranges Federations" aims at enhancing the European cyber ranges capability by federating existing national cyber ranges into a larger cluster with more capacity and unique services. This correspondingly enables sharing and pooling the capabilities and improving the quality of cyber training and exercises as well as using the federation for cyber-related research and development purposes.

The EDA kept looking at possible implications of hybrid threats for military capability development and associated requirements, based on the 2018 **Capability Development Plan** (CDP) revision. Specifically, the **EU Capability Development Priorities**, which contribute to countering hybrid threats, are enabling capabilities for cyber responsive operations, ground combat capabilities, underwater control contributing to resilience at sea, air superiority and cross-domain capabilities to achieve the EU's level of ambition with a focus on innovative technologies for enhanced future military capabilities including the CBRN-E.

In 2021, a research project called **Stand-off Detection of Hybrid Threats Containing Explosives** (STYX) was initiated by the EDA, aiming at developing and test systems for detecting and identifying explosive threats. Besides a technology survey of potential suitable technologies, the project will also perform realistic test and evaluation of emerging detection techniques, in accordance with operational hybrid warfare scenarios.

On 15 February 2022, the **Commission published its communication on its support to European defence**[61]. With this communication, the Commission is further contributing to the aims and goals of the Strategic Compass.

The **European Defence Fund (EDF)**[62] – with a budget close to EUR 8 billion for 2021-27 – keeps contributing to establishing a European defence ecosystem capable of delivering state of the art interoperable defence technologies and equipment that will enhance the Union's freedom of action and its technological sovereignty and competitiveness, thus increasing strategic resilience and security of supply.

[60] These are Main Battle Tank, Soldier Systems, European Patrol Class surface ship, Anti Access Area Denial capacities and Countering Unmanned Aerial Systems, Defence in Space and Enhanced Military Mobility.
[61] COM(2022) 60 15.2.2022
[62] Regulation (EU) 2021/697 of the European Parliament and of the Council of 29 April 2021 establishing the European Defence Funds and repealing Regulation (EU) 2018/1092, OJ L170, 12.5.2021, p. 149-177.

Moreover, on 18 May 2022, the Commission and the High Representative also presented a **Joint Communication on defence investment gaps and the way forward**[63]. This Joint Communication came about as a consequence of Russia's war of aggression against Ukraine and the new security environment. It looks into defence investment gaps and proposes further initiatives to strengthen the European Defence Industrial and Technological Base (EDTIB). Amongst others, it proposes a defence joint procurement task force, in particular to support coordination for very short-term procurement needs; a short-term EU instrument (with EUR 500 million over 2 years) to support joint procurement to address urgent needs; and a European Defence Investment Programme (EDIP) Regulation.

Protecting public health and food security

As part of ongoing and planned efforts to improve awareness of and resilience to hybrid threats within existing preparedness and coordination mechanisms, the Health Security Committee in the Commission kept tackling disinformation about COVID-19 in its Communication Network where it also addresses broader vaccine hesitancy issues. The unprovoked Russian war of aggression against Ukraine has further destabilised already fragile agricultural markets. Together with the Covid-19 pandemic and climate change, agriculture is under significant pressure, threatening food security worldwide.

The resilience of the agricultural sector during the COVID-19 pandemic shows that the EU has policies and tools to formulate crises response. The EU aims to reinforce the common understanding on key principles to follow in times of crises and to enhance preparedness protocols. Concretely, the main instrument to improve coordination in times of food security crisis was the setting up in November 2021 of a group of experts on the **European Food Security Crisis Preparedness and Response Mechanism** (EFSCM), including public and private actors. This forum allows for exchanges on preparedness activities on a regular basis and for a closer and quicker coordination and exchange of information between all actors in times of a crisis. The official launch of the EFSCM was organised in March 2022, as well as the first extraordinary gathering of the expert group in crisis mode due to the Russian war of aggression against Ukraine.

In order to protect food security in the EU and ensure resilience of the sector, and as announced in the Communication of the European Commission for Safeguarding food security and reinforcing the resilience of food systems[64] adopted on 23 March 2022, the European Commission will propose that Member States share reliable information on private stocks of essential food and feed in order to have a timely and accurate overview of their availability.

Russia's war of aggression against Ukraine has also raised the issue of weaponisation of food. Cutting off Ukrainian access to the Black Sea trading routes has effectively blocked Ukraine's exports of grain, and deliberately seizing and destroying agricultural machinery, fertilizer, seeds and agricultural fuel stocks in Ukraine are examples of using food as a weapon by Russia. In order to be further prepared to counter such threats on global food security, the EU in collaboration with third countries and international organisations, such as the UN and the Food and Agriculture Organization (FAO), must actively engage in diplomatic efforts to ensure an EU Global Food Security Response. The EU has been vocal in denouncing the weaponisation of food security by Russia and has been actively fighting mis- and disinformation about Russia's role in generating this crisis.

[63] JOIN(2022) 24 final
[64] COM(2022) 133 final

Furthermore, since 2019, the EU has reinforced and strengthened components of its **disaster risk management.** The upgraded EU Civil Protection Mechanism (UCPM) established a new European reserve of additional capacities (the 'rescEU reserve'), which complements (as a "last resort" instrument) the capacities available at national level and those included in the European Civil Protection Pool (ECPP). The rescEU capacities will include, among others, firefighting planes and helicopters, medical evacuation capacities, medical stockpiles, emergency medical teams, and capacities to address chemical, biological, radiological and nuclear or explosive (CBRN) hazards and threats. Through the strengthened UCPM, the EU will therefore be better prepared and respond to different types of emergencies, such as forest fires, medical emergencies or chemical, biological, radiological, and nuclear incidents.

At the end of the reporting period, nine Member States were hosting rescEU medical stockpiles of personal protective equipment (PPE) and intensive care equipment, and a consortium of 10 Member and Participating States have agreed on the technical characteristics and composition of a future rescEU Emergency Medical Teams (EMT) capacity. The objective is to develop three fully interoperable EMT type 2 (EMT2) capacities with a number of potential specialised care teams. The relevant implementing act was adopted on 22 February 2022[65].

CBRN related risks

Following the development of the **list of high-risk chemicals** that are of most concern in terms of use for terrorist purposes, the Commission conducted a study on the feasibility of restricting access to certain high-risk chemicals, which was finalised in May 2021. The findings of the study were shared with Member States experts in the CBRN Advisory Group where the Commission received support to continue with a robust impact assessment. In line with this, the Commission started working on an impact assessment for a possible proposal regulating the marketing and use of high-risk chemicals in the Union.

The Commission is continuing the **chemical detection trials** in cooperation with law enforcement authorities and networks. Several guidance materials have already been developed, covering chemical, radiological and explosives threat. These documents target specific users and environments, e.g. rail police or in-flight security officers.

The EDA's CapTech CBRN & Human Factors launched a **CBRN Framework Service Contract for the development of studies, reports and demonstrators** in 2020 and the associated activities are ongoing. The first three specific contracts address Personal Protective Equipment, Detection Identification and Monitoring of CBRN and Protection of Critical Infrastructure from CBRN. The review of the scenarios related to CBRN hybrid threats commenced in the third quarter of 2021 and are expected to be finalised during the third quarter of 2022.

The **European Defence Fund** addresses CBRN on a continuous basis, in particular financially supporting research and development projects on military CBRN systems and defence medical countermeasures. In 2021, the EDF allocated EUR 18.5 million to research on the detection and identification of CBRN threats as well as EUR 50 million to the development of defence medical countermeasures.

[65] Commission Implementing Decision (EU) 2022/288 of 22 February 2022 amending Implementing Decision (EU) 2019/570 as regards rescEU shelter capacities and the modification of quality requirements for Emergency Medical Teams Type 3 capacities (notified under document C(2022) 963), OJ L43, 24.2.2022, p/ 68-72.

Furthermore, the Commission together with Member States and Participating States of the UCPM are in the process of establishing rescEU capacities for CBRN decontamination, CBRN stockpiles and for CBRN detection, sampling, identification and monitoring capacities. Finally, to prepare for and respond to radiological and nuclear events, the European Anthropogenic Scientific Partnership, which provides 24/7 scientific advice to the European Response Coordination Centre (ERCC), was established.

EU support continued to be available to the majority of the European Neighbourhood Policy (ENP) partners within the framework of the EU CBRN Centres of Excellence (CoE) Initiative, with the aim of tackling CBRN risks of a natural, accidental or malevolent nature on a regional or trans-regional scale. In the ENP regions, the focus was on capacity building activities to reinforce border controls, first response, forensics analysis, adequate management of CBRN waste, medical and civil protection capacities adapted to CBRN incidents. EU CBRN CoE support also remained relevant in addressing the COVID-19 pandemic.

Cybersecurity

Closer operational cooperation between Member States and EU institutions, bodies and agencies, including all communities (resilience, law enforcement, cyber diplomacy, and cyber-defence) responsible for cybersecurity, is more vital than ever. The co-legislators reached a political agreement on the revised Directive on Security of Network and Information Systems ("the NIS 2 Directive") in May 2022, which gives the European Cyber Crises Liaison Organisation Network (EU - CyCLONe) a formal legal basis.

The agreed new rules raise the EU common level of ambition on cyber-security through a wider scope, clearer requirements for companies and provide for stronger supervision tools. The NIS 2 Directive covers medium and large entities from more sectors that are critical for the economy and society, including providers of public electronic communications services, more digital services such as social platforms, waste water and waste management, manufacturing of critical products, postal and courier services and public administration, both at central and regional level. The NIS 2 Directive also strengthens cybersecurity requirements imposed on companies, addresses security of supply chains and supplier relationships and introduces accountability of top management for non-compliance with the cybersecurity obligations. It streamlines reporting obligations, introduces more stringent supervisory measures for national authorities, as well as stricter enforcement requirements, and aims at harmonising sanctions regimes across Member States. It will help increase information sharing and cooperation on cyber crisis management at a national and EU level.

Another important aspect in improving cybersecurity is the security of digital products that companies and consumers are increasingly relying upon, which will be tackled by the Cyber Resilience Act (CRA), planned for September 2022. The CRA would mandate cybersecurity requirements for digital products before their placing on the internal market and also throughout the product lifecycle (e.g. maintenance, security updates). This would include both tangible and intangible digital products, such as stand-alone software. It would contribute to further strengthening supply chain security.

Since the Commission's Recommendation on building a **Joint Cyber Unit** (JCU), discussions have intensified on a structure for coordinated cooperation at operational and tactical level. On 19 October 2021, the Council agreed to explore the potential of the JCU initiative complementing the Commission's Recommendation on a coordinated response to large-scale

cybersecurity incidents and crises, and further guidance was provided under the Slovenian Presidency of the Council on the way forward[66].

In line with the objective of further strengthening the cyber crisis mechanisms, the **EU Cyber Crisis Linking Exercise on Solidarity** (EU CyCLES), organised by the French Presidency in cooperation with the High Representative and the EU Cybersecurity Agency (ENISA), tested the cooperation between operational and political levels and gave a European dynamic to solidarity and mutual assistance in case of a large-scale cyber incident. It further allowed the exploration of interactions between the internal and external aspects of response to incidents.

ENISA and CERT-EU have published **guidelines** on how to increase resilience and preparedness in the EU[67]. These encourage all public and private sector organisations in the EU to adopt a minimum set of cybersecurity best practices with a view to substantially improving cybersecurity culture.

On 9 March 2022, building on the aforementioned joint publication, with ENISA's support, CERT-EU published a follow-up technical guidance urging all organisations in the EU to apply it[68]. The recommendations therein would allow organisations to improve their cybersecurity posture and detect and react to cyber operations that may be carried off by sophisticated threat actors.

On 3 March 2022, CERT-EU also published a security guidance for hardening the configuration of Signal apps[69]. The document provides clear and pragmatic recommendations and is addressed to staff of both public and private organisations, including senior management, that may be using Signal for work-related matters or business continuity purposes, in case other tools of communication become unavailable.

For the years 2021 and 2022, **Horizon Europe** provides funding for research on cybersecurity with the explicit goal of creating robust digital infrastructures capable to resist and counter cyber-attacks and hybrid threats. More specifically, funded research should contribute to strengthening the EU's cybersecurity capacities and its sovereignty in digital technologies as well as creating more resilient digital infrastructure, systems and processes.

Under the first work programme 2021-2022 of Horizon Europe, funding was allocated from the cluster ''Civil Security for Society' to 15 projects, which are meant to help increase the capacity of practitioners in countering cyberattacks. These projects will also contribute to fostering the implementation of the new EU Cybersecurity Strategy (2020)[70].

Regarding the **cybersecurity of 5G networks**, while work is still ongoing in some Member States, a vast majority of them have already reinforced or are in the process of reinforcing security requirements for 5G networks based on the EU toolbox, including putting in place frameworks for imposing appropriate restrictions on 5G suppliers considered to be high-risk. Requirements on mobile network operators are being reinforced through the transposition of the Electronic Communications Code, and the EU Agency for Cybersecurity (ENISA) is preparing a candidate EU cybersecurity certification scheme for 5G networks.

[66] Council Conclusions on exploring the potential of the Joint Cyber Unit initiative - complementing the EU Coordinated Response to Large-Scale Cybersecurity Incidents and Crises, 12534/21, 8 October 2021
[67] https://www.enisa.europa.eu/publications/boosting-your-organisations-cyber-resilience
[68] Security Guidance 2022-01 - Cybersecurity mitigation measures against critical threats.
[69] CERT-EU Security Guidance 22-002 - Hardening Signal
[70] https://digital-strategy.ec.europa.eu/en/policies/cybersecurity-strategy

In addition, on 11 May 2022 Member States, with the support of the Commission and ENISA, published a report on the **cybersecurity of Open Radio Access Networks ('Open RAN')[71].** In the coming years, Open RAN will provide an alternative way of deploying the radio access part of 5G networks based on open interfaces. The report concludes that, although Open RAN could bring security opportunities in the future, for the time being it lacks maturity and creates significant risks, especially in the short-term. The report recommends a set of actions to help mitigate these risks and a cautious approach to deploying this new architecture.

In January 2022, the Commission adopted a Delegated Regulation[72] rendering applicable certain essential requirements of the **Radio Equipment Directive**[73] **(RED)**, more specifically those that address elements of cybersecurity risks, such as protection of privacy and protection from fraud to the manufacturers for certain categories of wireless devices. The obligations include the implementation of technical measures to these products so that the overall level of cybersecurity is increased. It will be applicable as of 1 August 2024. In the meantime, the European Standardisation Organisation will develop harmonised standards in support of the aforementioned legislation so that they can provide presumption of conformity if applied by the manufacturers.

The European Cybersecurity Competence Centre (ECCC) and Network of National Coordination Centres (NCCs)

The Regulation establishing the **European Cybersecurity Competence Centre (ECCC) and Network of National Coordination Centres (NCCs)** entered into force on 28 June 2021[74]. The ECCC, together with the Network of NCCs, is Europe's new framework to support innovation and industrial policy in cybersecurity. This ecosystem will strengthen the capacities of the cybersecurity technology community, shield our economy and society from cyberattacks, maintain research excellence and reinforce the competitiveness of EU industry in this field. The Centre and the Network will make strategic investment decisions and pool resources from the EU, its Member States and, indirectly, industry to improve and strengthen technology and industrial cybersecurity capacities, enhancing the EU's open strategic autonomy. The Centre will play a key role in delivering on the ambitious cybersecurity objectives for a Digital Europe.

Cybersecurity in the transport sector

In October 2021, the Commission made its **transport cybersecurity toolkit**[75] available in all official EU languages. The aim of this toolkit, which had been previously published in English only, is to raise awareness on cyber-risks and build preparedness in the transport sector. This toolkit contains recommended practices to mitigate some of the cyber threats that may affect the transport sector.

---

[71] https://digital-strategy.ec.europa.eu/en/library/cybersecurity-open-radio-access-networks

[72] Commission Delegated Regulation (EU) 2022/30 of 29 October 2021 supplementing Directive 2014/53/EU of the European Parliament and of the Council with regard to the application of the essential requirements referred to in Article 3(3), points (d), (e) and (f), of that Directive C/2021/7672, OJ L 7, 12.1.2022, p. 6–10.

[73] Directive 2014/53/EU of the European Parliament and the Council of 16 April 2014 on the harmonisation of the laws of the Member States relating to the making available on the market of radio equipment and repealing Directive 1999/5/EC, OJ L 153, 22.05.2014, p. 62-106.

[74] Regulation (EU) 2021/887 of the European Parliament and of the Council of 20 May 2021 establishing the European Cybersecurity Industrial, Technology and Research Competence Centre and the Network of National Coordination Centres, OJ L 202, 8.06.2021, p. 1-21.

[75] https://ec.europa.eu/transport/themes/security/cybersecurity_en

The Commission continued to ensure compliance with the cybersecurity-related obligations under existing **EU maritime security legislation**[76]**.** EMSA continued to follow cybersecurity aspects affecting the maritime domain closely. EMSA cooperates closely with ENISA and the European Coast Guard Functions Forum (ECGFF) on various issues related to maritime cybersecurity risks in order to provide Commission and Member States with technical support to understand and address maritime cyber risks better. ENISA has also published a new online tool to help ports identify and prioritise cybersecurity measures according to their own needs.

The Commission organised a workshop on cybersecurity in the maritime sector in December 2021 to allow various actors to present their initiatives in the area and to explore possible next steps, such as developing guidance on how to address cybersecurity for ships.

In relation to the EUMSS, the Commission continues to promote a comprehensive approach to maritime security risk management, in particular by conducting common risk analysis and identifying possible gaps and overlaps in this domain, while also taking into account cyber and hybrid threats, climate challenges and maritime environmental disasters.

In the rail sector, cybersecurity has been identified as one of four priority areas in the 2022 Work Programme of the working party on rail security under the Commission expert group on land transport security (LANDSEC). The Commission is actively supporting an exchange of information and good cybersecurity practice.

In the aviation sector, the implementation of aviation security legislation to address cybersecurity[77] was supported by Information Notes to help Member States' authorities and industry through providing guidance and best practices. The Commission organised meetings of the EU Aviation Cybersecurity Working Group bringing together aviation and cybersecurity experts to discuss topical issues of cybersecurity in the aviation sector. EASA through its European Strategic Cybersecurity Platform (ESCP) continued to implement the EU Cybersecurity in Aviation Strategy[78]. On 11 June 2021, EASA published an Opinion with provisions for the management of information security risks by competent authorities and organisations in all the aviation domains[79], with the objective to efficiently contribute to the protection of the aviation system from threats and consequences to cyber- and information security. In anticipation of the adoption of the new information security management system legal framework, EASA will be working on developing an implementation support roadmap, in coordination with the European Strategic Coordination Platform (ESCP) to assist the industry and authorities with their efforts and ensure effective implementation of the future rules.

[76] Regulation (EC) No 725/2004 of the European Parliament and of the Council of 31 March 2004 on enhancing ship and port facility security, OJ L 129, 29.04.2004 p. 6-91.
[77] Commission Implementing Regulation (EU) 2019/1583 of 25 September 2019 amending Implementing Regulation (EU) 2015/1998 laying down detailed measures for the implementation of the common basic standards on aviation security, as regards cybersecurity measures, OJ L 246, 26.09.2019, p. 15-18.
[78] https://www.easa.europa.eu/downloads/103075/en
[79] Opinion No 03-2021: DOA holders and POA holders, AOC holders (CAT), maintenance organisations, CAMOs, training organisations, aero-medical centres, operators of FSTDs, ATM/ANS providers, U-space service providers and single common information service providers, aerodrome operators and apron management service providers. The objective is to efficiently contribute to the protection of the aviation system from cybersecurity (information security) attacks and their consequences. These provisions include high-level, performance-based requirements for an information security management system that will be supported by AMC & GM and industry.

The Commission made a legislative proposal on a new Implementing Regulation[80] and a new Delegation Regulation[81] on Information Security Management, which is being discussed by the co-legislators with a view to its adoption in 2022. The European Centre for Cyber Security in Aviation (ECCSA) continued to operate as a platform for information sharing, threat analysis and standardisation. Moreover, the Network of Cybersecurity Analysts established by EASA started its activities to raise awareness of the importance of cybersecurity risks in civil aviation and support Member States to analyse information security incidents that have an impact on or could potentially affect aviation safety.

The European Aviation Crisis Coordination Cell (EACCC), established in 2011 in the aftermath of the volcanic ash crisis, continues to train, monitor and coordinate responses to any future aviation network crisis.

The Commission, assisted by EASA, actively participated in international fora managed by the International Civil Aviation Organisation (ICAO), the European Civil Aviation Organisation (ECAC) and Eurocontrol to contribute to their work on further developing policies and cooperation at multilateral and European levels in the area of aviation cybersecurity.

In terms of developing aviation security capacity in third countries, the CASE II project (Civil Aviation Security in Africa, the Middle East and Asia) aims at improving the aviation security ecosystem in partner countries and it includes a component on cybersecurity capacity building, based on the standards set out by ICAO.

Cybersecurity in the energy sector

The Commission continued working in close collaboration with ENISA and the dedicated sectorial work stream on energy of the **NIS Cooperation Group** to ensure sectorial awareness and cooperation on sector specific topics.

Furthermore, **capacity building activities** with international partners are ongoing in order to reinforce their ability to address cyber threats to targeting critical infrastructure.

Cybersecurity in the financial services sector

In January 2022, the European Systemic Risk Board (ESRB) published a **Recommendation for the establishment of a pan-European systemic cyber incident coordination framework** (EU-SCICF). The EU-SCICF aims to strengthen the coordination among financial authorities in the EU, as well as with other authorities in the EU and key actors at

[80] Commission Implementing Regulation introducing requirements for the management of information security risks with a potential impact on aviation safety for organizations covered by Commission Regulations (EU) No 1321/2014, No 965/2012, No 1178/2011, 2015/340, 2017/373 and 2021/664, and for competent authorities covered by Commission Regulations (EU) No 748/2012, No 1321/2014, No 965/2012, No 1178/2011, 2015/340, 2017/373, No 139/2014 and 2021/664 and amending Commission Regulations (EU) No 748/2012, No 1321/2014, No 965/2012, No 1178/2011, 2015/340, 2017/373, No 139/2014 and 2021/664 as regards the introduction of requirements for the management of information security risks with a potential impact on aviation safety.

[81] Commission Delegated Regulation introducing requirements for the management of information security risks with a potential impact on aviation safety for organizations covered by Commission Regulations (EU) No 748/2012 and No 139/2014 and amending Commission Regulations (EU) No 748/2012 and No 139/2014 as regards the introduction of requirements for the management of information security risks with a potential impact on aviation safety for organizations

international level. It would complement the existing EU cyber incident response frameworks by addressing the risks to financial stability stemming from cyber incidents.

On 11 May 2022, the Council Presidency and the European Parliament reached a provisional agreement on the **Digital Operational Resilience Act (DORA)**[82]. The aim is to create a regulatory framework on digital operational resilience whereby all firms need to make sure they can withstand, respond to and recover from all types of ICT-related disruptions and threats.

Cyber defence

In line with the ambition set out in the Strategic Compass to better protect, detect, defend and deter against cyberattacks, the development of the EU's Cyber Defence Policy document begun in 2022. Further development of EU's Cyber Defence Policy will boost research and innovation, stimulate the EU's industrial base and promote education and training to ensure that we are ready to act. It will increase cooperation among the EU's and Member States' cyber defence actors and develop mechanisms for leveraging capabilities at the EU level, including in the context of CSDP missions and operations. It will also strengthen cooperation with like-minded partners in the area of cyber defence, notably NATO.

On 15 September 2021, the EU Military Committee (EUMC) approved the EU Military Vision and Strategy on Cyberspace as a Domain of Operations, that sets the framework conditions and describes the ends, ways and means needed to use cyberspace as a domain of operations in support of CSDP military missions and operations. On 4 May 2022, the EUMC approved the Concept on Cyber Defence for EU-led military missions and operations. This concept provides Member States, framework nations, troop contributing nations and EU military organisations with up-to-date generic principles, procedures, roles and responsibilities. This is to support the efficient planning and provision of cyber defence activities in order to protect, defend and support CSDP military missions and operations across all domains.

Pooling and sharing of training and exercises is a key success factor for cyber defence. EDA continues to further develop and run pilot courses and exercises for new training formats and delivers a variety of **new cybersecurity & defence courses.** Cyber Phalanx 2021, a one-week combined course and exercise for operations planners, was successfully concluded in Lisbon, Portugal in September 2021. In January 2022, EDA also organised the second-ever live-fire cyber exercise specifically dedicated to improving European cooperation between Member States' national military Computer Emergency Response Teams (CERTs)[83].

A number of Member States are developing and contributing to cyber defence-related projects under the **Permanent Structured Cooperation** (PESCO).

As regards the **cyber training plan**, established in the European Security and Defence College (ESDC) and implemented with the support of EDA and ESDC's network partners, the 'Cyber Implications to CSDP Operations and Missions Planning Course' took place in Brussels in June 2022.

To respond to the need to increase investments and strengthen capabilities, which were addressed in the Strategic Compass, joint defence R&D projects are supported through the

[82] Digital finance: Provisional agreement reached on DORA - Consilium (europa.eu)

[83] The exercise gathered more than 200 experts from 19 EDA Member States and Switzerland, all of them connecting remotely. The objective of the exercise was to bring together military CERTs and observe incident management dynamics with a particular focus on information sharing, a key factor in modern cyber defence.

EDF. In the 2021 EDF budget, more than EUR 33 million was reserved for proposals for increased cyber capabilities, focusing on improved cyber operations and cyber training. The EDF work-programme for 2022, which was adopted on 25 May 2022, with a budget EUR 70 million for cyber defence, contains one research call on adapting cyber situational awareness and one development call with topics addressing cyber and information warfare toolbox and cybersecurity and systems for improved resilience.

Over the reporting period, **cooperation activities between** ENISA, CERT-EU, EDA and the European Cybercrime Centre of Europol (EC3) in the framework of the joint memorandum of understanding, signed in 2018, continued.

Cyber defence is also a priority of ongoing cooperation between the EU and NATO.

Gathering electronic evidence

The Commission continued to facilitate the negotiations between the European Parliament and the Council as part of the EU-legislative procedure on the Commission's April 2018 e-evidence proposals[84]. The **e-evidence proposals** aim to improve cross-border access to electronic evidence for criminal investigations and are needed by law enforcement and judicial authorities to ensure they can respond to terrorism and other serious crimes, including the increasing threat of cybercrime.

Framework for a Joint EU Diplomatic Response to Malicious Cyber Activities (the "cyber diplomacy toolbox"), including an EU horizontal cyber sanctions regime

The *Framework for a Joint EU Diplomatic Response to Malicious Cyber Activities*[85] (the "**cyber diplomacy toolbox**") is part of the EU's wider approach to cyber diplomacy, which contributes to conflict prevention, the mitigation of cybersecurity threats and greater stability in international relations. On 23 March 2022, the Council adopted Conclusions on the development of the EU's cyber posture[86], which highlights the five functions of the EU in the cyber domain.

In line with the ambition set out under the 2020 Joint Communication on the EU's Cybersecurity Strategy[87] and the Strategic Compass, the EU and Member States continuously work to improve the EU's ability to prevent, discourage, deter, and respond to malicious cyber activities. In this regard, the EU and Member States are working to strenghten their cyber posture, explore additional measures to the cyber diplomacy toolbox, further step-up cooperation with like-minded partners, including NATO, and integrate cyber within the broader security and defence policy, including through regular exercises.

The **EU has responded to malicious cyber activities on multiple occasions**, notably through several public statements as well as listings under the EU autonomous horizontal cyber sanctions regime. Most recently on 14 January 2022, the High Representative published a declaration on behalf of the EU strongly condemning the cyber-attacks against Ukraine,

[84] Proposal for a Regulation of the European Parliament and of the Council on European Production and Preservation Orders for electronic evidence in criminal matters, COM/2018/225 final and Proposal for a Directive of the European Parliament and of the Council laying down harmonised rules on the appointment of legal representatives for the purpose of gathering evidence in criminal proceedings, COM/2018/226 final.
[85] Framework for a Joint EU Diplomatic Response to Malicious Cyber Activities (the "cyber diplomacy toolbox"), 9916/17, 19 June 2017
[86] Council Conclusions on the development of cyber posture, 9364/22, 23 May 2022.
[87] JOIN(2020) 18 final

demanding the cyber-attacks be put to an end immediately, and expressing solidarity and support for Ukraine[88]. In addition, on 10 May 2022, the High Representative published a declaration on behalf of the EU attributing the cyber-attack, which targeted the satellite KA-SAT network one hour before Russia's war on aggression against Ukraine on 24 February 2022 started, to Russia, and on 19 July the High Representative issued a declaration on malicious cyber activities conducted by hackers and hacker groups in the context of Russia's aggression against Ukraine[89]. Further diplomatic measures to respond to cyber threats and attacks targeting Ukraine were integrated within the EU's wider response to Russia's war of aggression against Ukraine. Individuals, entities and bodies are currently listed under the EU cyber sanctions regime for being responsible or involved in significant cyber-attacks with a significant effect, which constitute an external threat to the Union or its Member States. The EU cyber sanctions regime was renewed until May 2025, and the restrictive measures set out therein until 2023[90].

Since the beginning of Russia's war of aggression against Ukraine, the EU is closely monitoring the cyber threat landscape. The EU together with its Member States continued to provide further support in relation to cyber attacks, in the form of equipment, software and services, based on urgent requests by Ukraine. Furthermore, the EEAS, in cooperation with the Commission services, Member States and like-minded partners, has established a clearing house to coordinate short-term cyber assistance to Ukraine. Finally, work continues in relation to enhancing security and cyber support to Moldova and Georgia, as well as partners in the Western Balkans, by exploring measures to be mobilised rapidly to support strengthening cyber resilience in these countries.

International cooperation in cybersecurity

With the evolving tensions in cyberspace, including governance of cyberspace, the EU and its Member States stepped up their efforts, notably through **discussions in the United Nations and other relevant international fora,** to promote the strategic framework for conflict prevention, stability and cooperation in cyberspace. Together with 32 other States, the EU and its Member States are working to **establish a Programme of Action (PoA) to Advance Responsible State Behaviour in cyberspace**, which offers a permanent platform for cooperation and exchange of best practices within the UN, and proposes to establish a mechanism to put in practice the norms of responsible state behaviour and promote capacity building. The work under the PoA builds on the 2010, 2013, 2015 and 2021 UN Group of Governmental Experts (UNGGE) reports that outline the strategic framework for conflict prevention, stability and cooperation in cyberspace, and the endorsement of that framework in the 2021 Open-ended Working Group (OEWG) consensus report[91]. The Cyber PoA will make use of the outcome of the sixth UNGGE that concluded a consensus report in May 2021[92] and will seek synergies with the second OEWG currently in place. With these efforts, the EU and its Member States continue to strongly promote a global, open, free, stable and secure

[88] https://www.consilium.europa.eu/en/press/press-releases/2022/01/14/ukraine-declaration-by-the-high-representative-on-behalf-of-the-european-union-on-the-cyberattack-against-ukraine/

[89] https://www.consilium.europa.eu/en/press/press-releases/2022/07/19/declaration-by-the-high-representative-on-behalf-of-the-european-union-on-malicious-cyber-activities-conducted-by-hackers-and-hacker-groups-in-the-context-of-russia-s-aggression-against-ukraine/

[90] Council Decision (CFSP) 2022/754 of 16 May 2022 amending Decision (CFSP) 2019/797 on restrictive measures against cyber-attacks threatening the Union or its Member States, OJ L138, 17.5.2022, p. 16.

[91] https://front.un-arm.org/wp-content/uploads/2021/03/Final-report-A-AC.290-2021-CRP.2.pdf

[92] Report of the Group of Governmental Experts on Advancing responsible State behaviour in cyberspace in the context of international security, 28 May 2022.

cyberspace, respecting human rights and fundamental freedoms, supporting social, economic and political development worldwide.

Taking into account the global and evolving nature of hybrid threats, building and maintaining robust alliances and partnerships with third countries is fundamental to advancing international stability and security in cyberspace. The EU has established specific **cyber dialogues** with the United States, Japan, Brazil, India, South Korea and China. In 2021, the first EU-Ukraine Cyber Dialogue took place, allowing to further deepen the cooperation with Ukraine on the full range of cyber issues. Furthermore, the EU seeks to strengthen its consultations with other partners, including regional and international organisations such as the Organisation of American States (OAS), African Union (AU), ASEAN Regional Forum (ARF), the Organisation for Security and Cooperation in Europe (OSCE) and NATO.

Screening of foreign direct investment (FDI)

The **FDI Screening Regulation**[93] entered fully into effect on 11 October 2020 and has already demonstrated real added value with the new cooperation mechanism between Member States and the Commission, and the sharp increase in Member States with a national mechanism in place (or likely to be adopted shortly).

Building resilience against radicalisation and violent extremism

Radicalisation and violent extremism increasingly have a cybersecurity and digital dimension. The increased use by terrorist groups of information and communication technologies for planning and perpetrating terrorist attacks, and the risks of potential use of emerging technologies by terrorist entities increase the need for EU action in this domain. On the other hand, new technologies offer potential to tackle terrorist threats.

Based on the transnational nature of radicalisation and violent extremism, cooperation with partners is key to address these challenges. For the cybersecurity and digital dimension, capacity building and exchanges with partner countries to maximise the benefits of new technologies for security services and to counter terrorists' misuse of new technologies are encouraged. Work is ongoing to plan for actions that include support for capacity building with regard to new technologies in the field of analysis of information.

Research and innovation play a key role in reinvigorating the resilience and countering extremism. The first work programme 2021-2022 of Horizon Europe under the cluster 'Civil Security for Society' provides funding to actions analysing the evolution of political extremism and its influence on contemporary social and political dialogue.

The **EU Strategic Orientations on a coordinated EU approach to prevention of radicalisation for 2022 and 2023**[94] focuses on several activities that contribute to increasing resilience, strengthening Member States' capacities in strategic communications and preventing radicalisation. This includes fighting conspiracy theories, responding to emerging hybrid ideologies as well as addressing undesirable foreign influence fuelled by funding. The Commission further works to prevent risks inherent with in-home schooling and other forms of non-formal education, including online, and focuses on prevention of radicalisation among

[93] Regulation (EU) 2019/452 of the European Parliament and of the Council of 19 March 2019 establishing a framework for the screening of foreign direct investment in the EU, OJ L 791, 23.3.2019, p. 1-14

[94] https://ec.europa.eu/home-affairs/system/files/2022-03/2022-2023%20Strategic%20orientations%20on%20a%20coordinated%20EU%20approach%20to%20prevention%20of%20radicalisation_en.pdf

vulnerable groups, in particular youth and children. It further includes supporting Member States in translating successful prevention and countering violent extremism initiatives into the online world.

The **EU Regulation to address the dissemination of terrorist content online**[95] has been applicable since 7 June 2022. It increases powers of national competent authorities to curb the spread of terrorist content, including messages that incite violence, recruit individuals and glorify terrorist attacks, thereby preventing radicalisation.

The European Commission's **EU Internet Forum**[96] continues to provide a platform for voluntary collaboration with the technology industry to respond to emerging challenges online. The EU Internet Forum distributed the first Knowledge Package on violent right-wing extremist groups, symbols and manifestos to companies to support their voluntary content moderation efforts. An updated version will be produced in 2022. In the framework of the EU Crisis Protocol[97], work is ongoing to improve strategic crisis communication by Member States in case of terrorist attacks to build resilience against misinformation.

The EU Internet Forum is further organising technical meetings on the risks related to algorithmic amplification and borderline content disseminating violent extremist ideologies and addresses financing of violent extremism and terrorism with an online perspective. It expands its outreach to additional members of industry by addressing terrorist-operated websites. The Forum continues to enhance the resilience of the online video-gaming community and provides alternative narratives to radicalised discourses and terrorist propaganda and promotes fundamental rights and values through the **Civil Society Empowerment Programmes** (CSEP).

Increasing cooperation with partner countries

In the framework of the implementation of Action 18 of the Joint Framework on countering hybrid threats, **Hybrid Risk Surveys** have been launched with seven partners: four in the Western Balkans (Albania, Kosovo[98], North Macedonia and Montenegro), two in the Eastern Neighbourhood (Moldova and Georgia), and one in the Southern Neighbourhood (Jordan). Based on the outcomes of these surveys, the EEAS and the Commission services agreed recommendations in priority domains with the partners. Support measures to mitigate risks have been provided through existing projects or support such as the European Commission's Technical Assistance and Information Exchange Instrument (TAIEX).

In 2021, despite the difficult context of the COVID-19 pandemic, a number of partners have received support via TAIEX on the domain of cybersecurity, strategic communication and critical information infrastructure[99]. Other TAIEX support measures are planned on

[95] Regulation (EU) 2021/784 of the European Parliament and of the Council of 29 April 2021 on addressing the dissemination of terrorist content online, OJ L 172, 17.05.2021, p. 79-109.
[96] https://ec.europa.eu/home-affairs/networks/european-union-internet-forum-euif_en
[97] https://ec.europa.eu/commission/presscorner/detail/en/ip_20_2372
[98] This designation is without prejudice to positions on status, and is in line with UNSCR 1244/1999 and the ICJ Opinion on the Kosovo declaration of independence.
[99] In July 2021, Moldova received a TAIEX expert mission on communication and negotiation in crisis situations. In December 2021, TAIEX supported Ukraine to develop new approaches of cooperation between relevant authorities of Ukraine and Member States in the migration sphere, in particular on combating irregular migration, readmission, document security and protection of refugees' rights; in 27 April 2022, a high-level online TAIEX Workshop on "The New Geopolitical Consequences of Disinformation in the Western Balkans" was organised; May 2022, Albania received a TAIEX Study Visit on Regulations and Operational Environment of a Cyber Security Authority.

cybersecurity, cyber incident preparedness and disinformation, especially given the urgent needs dictated by the latest developments in Ukraine.

Projects and other activities are also ongoing in partner countries, where relevant addressing the recommendations from the Hybrid Risk Surveys.

With respect to **the Western Balkans,** the Commission is currently overseeing the implementation of a regional identification and formulation study on cybersecurity. The Western Balkans were also invited as observers to the first meeting of the "**European Food Security Crisis Preparedness and Response Mechanism**" (EFSCM) which took place on 9 March 2022, with sectoral and national experts calling for action to allow flexibility in sourcing raw materials.

In the **Eastern Neighbourhood**, the EU funded the regional CyberEast programme. Capacity building and technical assistance continues to be provided to the EaP partners on cybersecurity and cybercrime.

In **Ukraine,** the Commission will provide approximately EUR 10 million under the Neighbourhood, Development and International Cooperation Instrument (NDICI) to improve Ukrainian cybersecurity and data security needs. This will be aimed towards supporting relevant Ukrainian beneficiaries to implement increased cybersecurity and data security in line with best practices and taking into account all standards that safeguard fundamental freedoms; and assuring the Ukrainian beneficiaries have an improved capacity to tackle cyber threats and secure data confidentiality, integrity and availability.

In December 2021, the Council adopted a set of measures under the European Peace Facility worth EUR 31 million to enhance the overall resilience of Ukraine and strengthen the capabilities of the Ukrainian Armed Forces, including support on cyber.[100]

On the cooperation with developing countries, the EU's ambitions and investments into cyber capacity-building are growing, building on the implementation of its 2013 Cybersecurity Strategy[101], which contributed to a more systematic linking of its action on external cyber capacity building.

Recently, an important part of the EU's work has focused **on Africa.** Africa is particularly vulnerable to malicious cyber activities by both state and non-state actors, which target vital internet infrastructure, thereby posing a threat to economies and democratic institutions and increasing the risk of political conflict. It is therefore particularly important for digital economic growth and development to go hand-in-hand with increased cybersecurity and resilience. Ongoing projects in Africa include the OCWAR-C (Organised Crime: West African response on Cybersecurity and fight against Cybercrime), planned for the 2018-2022 period[102].

EU Playbook and exercises

Following an agreement on the **new Parallel and Coordinated Exercises (PACE) plan,** with the EU as a leading organisation with the **EU Integrated Resolve 22 crisis**

[100] https://www.consilium.europa.eu/en/press/press-releases/2021/12/02/european-peace-facility-council-adopts-assistance-measures-for-georgia-the-republic-of-moldova-ukraine-and-the-republic-of-mali/

[101] Joint Communication to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions – Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace, JOIN(2013) 1 final, 7.2.2013.

[102] Participating countries are Benin, Burkina Faso, Cabo Verde, Cote d'Ivoire, The Gambia, Guinea, Guinea-Bissau, Liberia, Mali, Niger, Nigeria, Senegal, Sierra Leone and Togo, as well as Mauritania.

management exercise and NATO with the Crisis Management Exercise (CMX 23), preparations for the EU Integrated Resolve 2022 exercise are underway. The exercise will take place in autumn 2022.

In parallel, the review process on the **EU Playbook on countering hybrid threats is ongoing,** conducted by the Commission services, in cooperation with the EEAS.

Article 42(7) of the Treaty on European Union (TEU) and Article 222 of the Treaty on the Functioning of the European Union

Following a request from Member States to increase their common understanding of the implementation of Article 42(7) of the TEU, the EEAS, in consultation with the Commission services, produced a **non-binding overview on the implementation of Article 42(7) of the TEU**, which was discussed in the Political and Security Committee in January 2022. The overview outlines the scope of application, nature of aid and assistance, and a set of practical recommendations. It also outlines possible areas of support in its implementation, upon an explicit request by the attacked Member State. The Strategic Compass includes a commitment to continue regular exercises, including cyber exercises, and to explore its use in case of attacks originating from space or threats to space-based assets. The cyber exercises organised by the French Presidency and the High Representative, supported by ENISA, included the invocation of Article 42(7) of the TEU.

CSDP operations and missions

The Strategic Compass foresees that the EU hybrid toolbox must also include military actions and means for countering hybrid threats in CSDP missions and operations and in response to the needs of third countries in countering hybrid threats. Moreover, the EU Rapid Deployment Capacity (RDC) should be able to operate in a hybrid conflict environment. Based on that, an analysis of the military requirements, role and tasks in the context of the EU hybrid toolbox as well as the military contribution to the Hybrid Rapid Response Teams will be carried out and proposals made.

Regarding CSDP **military missions and operations,** the EU Military Staff (EUMS) continued to improve the delivery of key messages and raising awareness of the EU's CSDP missions and operations and their work on the ground. It has also continued the cooperation with NATO Public Affairs and Strategic Communications Advisor in order to highlight the added-value of EU-NATO cooperation. The EUMS and the Military Planning and Conduct Capability (MPCC) acted as a coordination link between the EU's CSDP missions and operation in matters of reporting and monitoring instances of disinformation.

Following the same EU integrated approach, the Civilian Planning and Conduct Capability (CPCC) continued the efforts to establish a dedicated hybrid capacity within its deployments, with a particular focus on strengthening the situational awareness at the mission level.

EU-NATO cooperation

Countering hybrid threats remains a key area of cooperation with NATO. Progress is steady, building upon the momentum established by the 2016 Warsaw Joint Declaration[103] and the 2018 Brussels Joint Declaration[104]. Details of notable interactions are contained in the

[103] https://www.consilium.europa.eu/media/21481/nato-eu-declaration-8-july-en-final.pdf
[104] https://www.consilium.europa.eu/media/36096/nato_eu_final_eng.pdf

Seventh Progress Report on the implementation of the common set of proposals presented by the High Representative of the Union for Foreign Affairs and Security Policy and the Secretary General of NATO to the respective Councils on 20 June 2022 [105]. Cooperation has continued on crisis response and bolstering resilience through reciprocal cross-briefings and regular staff-to-staff dialogue, as well as on **strategic communication and disinformation**, including in the context of the RAS and with the NATO Strategic Communications Centre of Excellence (StratCom CoE).

On **resilience**, the EU and NATO launched a **structured dialogue** in January 2022 focusing on topics of mutual interest. The first meeting covered, among other items, the resilience of critical infrastructure, and NATO's Baseline Requirements. The dialogue was continued in June 2022. In the context of the Russian war of aggression against Ukraine, exchanges at staff level were strengthened on critical infrastructure, cyber and **CBRN** threats, disinformation, security of supply and capacity building for partners.

Staff exchanges on **cyber issues** continue to take place, offering an opportunity to provide updates on respective policy developments and priorities, while assessing opportunities for further cooperation. In terms of strengthening cooperation on cyber exercises through reciprocal participation, CYBER PHALANX 21, an EU Command Post Exercise, held on 27 September – 1 October 2021, was opened for NATO staff participation in the planning and conduct phases. NATO representatives were also invited to observe the annual cyber diplomacy toolbox exercise CyDip TTX, held on 17 November 2021. The EDA took part in the planning and execution of exercise Locked Shields 2021 (organised by the NATO Cooperative Cyber Defence Centre of Excellence - NATO CCD CoE) in April 2021.

Cooperation in the area of **counter-terrorism (CT)** progressed well. Staff talks were held regularly, exchanging views on topics such as battlefield evidence, technical exploitation, capacity building for partners, countering improvised explosive devices, countering unmanned aerial systems, countering terrorist financing, and protection of critical infrastructure.

Within existing limitations of classified information sharing, the Hybrid Fusion Cell has maintained its **close cooperation with the NATO Hybrid Analysis Branch**.

Both the EU's Strategic Compass adopted by the Council on 21 March 2022 and NATO's new Strategic Concept, approved at the Madrid Summit on 29 June 2022, call for deepening the EU-NATO strategic partnership and increasing cooperation in countering hybrid threats.

Conclusion

The reporting period under review was marked by unprecedented changes and challenges in the hybrid threats landscape, most of all Russia's war of aggression against Ukraine and its global impact. At the same time, the COVID-19 pandemic and disinformation linked to it continued to have a major impact. Moreover, the EU faced new attempts to undermine its unity by instrumentalising migration flows. Due to the complexity and multifaceted nature of these challenges, the framework for countering hybrid threats and the whole-of-governance and whole-of-society approaches that are built into the policies have become even more relevant.

One of the most significant achievements during the reporting period has been the adoption of the Strategic Compass. It will offer the EU an opportunity to learn from and improve its

[105] eu-nato-progress-report.pdf (europa.eu)

mechanisms, tools and instruments to respond to complex changes in the threat landscape, including hybrid threats. In the framework of countering hybrid threats, the Strategic Compass will build upon the foundation that was set with the 2016 Joint Framework, 2018 Joint Communication, and the 2020 Security Union Strategy. This report outlines the broad range of measures that have already been taken across different domains.

In the framework of the Strategic Compass, during the reporting period, Member States have had active discussions on the setting up of an EU hybrid toolbox. The Commission services and the EEAS have supported these discussions actively. The EU hybrid toolbox aims to bring together the wide variety of different measures, tools and instruments that already exist and that will be developed in future. This will improve the coordination and coherence of the responses to hybrid threats in the future.

Cooperation with partners is key to countering hybrid threats efficiently. During the reporting period, cooperation with NATO has been deepened, with the setting up of a staff-to-staff EU-NATO structured dialogue on resilience, which should also contribute to improving resilience against hybrid threats. On the other hand, mostly due to the COVID-19 pandemic, the progress in supporting the EU's neighbours has been slower than anticipated in the framework of the Hybrid Risk Surveys. However, support through other means has been possible, and work to implement the recommendations from the Hybrid Risk Surveys or to relaunch the process is planned to continue.

Despite clear advances in many areas, and the prospect of an EU hybrid toolbox, work on countering hybrid threats needs to continue. The threat landscape is evolving, and thus the tools and instruments to protect the EU and its partners must also evolve. Russia's war of aggression against Ukraine clearly demonstrates the need to constantly adapt our tools and measures to respond to common threats.